240030

○新潟県警察情報セキュリティ対策要綱の制定について（例規通達）

情報管理課
平成17年２月18日
本部（情管）第５号

〔沿革〕　平成18年２月本部（情管）第11号、19年２月第４号、20年９月第45号、23年３月第26号改正

このたび、新潟県警察情報セキュリティに関する訓令（平成17年本部訓令第６号）に基づき、新潟県警察情報セキュリティ対策要綱を別添のとおり制定し、平成17年３月１日から施行することとしたので、誤りのないようにされたい。

なお、新潟県警察情報安全対策に関する訓令の制定について（平成13年９月21日付け本部（情管）第52号）及びＯＡ機器及びフロッピーディスク等管理要領の制定について（平成12年８月15日付け本部（情管）第54号）は、廃止する。

別添

新潟県警察情報セキュリティ対策要綱

第１　総則

１　趣旨

この要綱は、新潟県警察情報セキュリティに関する訓令（平成17年本部訓令第６号。以下「訓令」という。）に基づき、警察情報システム及び警察業務に係る情報の処理を行うその他の電子計算機（以下「警察情報システム等」という。）並びにそれらにおいて取り扱われる情報について、情報セキュリティの維持に関し、必要な事項を定めるものとする。

なお、県警察以外の機関が設置した電子計算機等のシステムの情報セキュリティの維持については、当該設置機関の定めによるほか、本要綱によるものとする。

２　用語の定義

この要綱における用語の意義は、訓令に定めるもののほか次に掲げるところによる。

(1)　アクセス

警察情報システム等にデータを入力し、又は警察情報システム等からデータを出力することをいう。

(2)　アクセス権者

アクセスを行う権限を与えられた者をいう。

(3)　アクセス範囲

アクセス権者ごとにその者が行うことができるアクセスの範囲をいう。

(4)　ユーザＩＤ

アクセス権者を識別するためにアクセス権者ごとに一意に付与された文字列をいう。

(5)　パスワード

警察情報システム等を利用しようとする者がアクセス権者本人であるかどうかを検証するため用いられる文字列をいう。

(6)　入出力資料

警察情報システム等に入力された又は警察情報システム等により出力された情報を記録した文書、図画及び電磁的記録（作成中のものを含む。）をいう。

(7)　ドキュメント

警察情報システム等に関する次に掲げる文書、図画及び電磁的記録（作成中のものを含む。）をいう。

ア　システムドキュメント

(ｱ)　システム仕様書

(ｲ)　システム設計書（情報の処理手順並びに機器及びプログラムの構成の概要の記録をいう。）

(ｳ)　プログラム仕様書（情報の処理手順の概要の記録をいう。）

(ｴ)　プログラムリスト

(ｵ)　操作指示書（システムの維持管理に伴う機器の設定方法等を説明した記録をいう。）

イ　取扱説明書

システムを利用する者が業務を行う上で参照する機器の操作の方法を説明した記録をいう。

(8)　警察情報セキュリティポリシー

訓令及び訓令に基づいて定められた情報セキュリティに関する事項をいう。

(9)　認証

ユーザＩＤ、パスワード等を警察情報システム等に入力することなどにより、アクセス権者が正当な者であるか否かを検証することをいう。

(10)　データベース装置

警察情報システム等を構成する汎用電子計算機、サーバ等の電子計算機及びこれらに附置されるシステム管理を行う電子計算機をいう。

(11)　ネットワーク機器

警察情報システム等を構成するルータ、レイヤ３スイッチ、スイッチングハブ等の機器若しくは伝送通信装置又はこれらから出力されるデータを利用することによりネットワークを管理する機能を有する機器をいう。

(12)　警察情報取扱機器

警察情報システム等で使用する機器のうち、警察情報システムで使用する機器を除いたものをいう。

(13)　持ち出し用パソコン

警察情報システム等のうち、一の警察の庁舎内から移動して運用するものとして整備したものをいう。

(14)　外部記録媒体

フロッピーディスク、フラッシュメモリ、ＤＶＤ規格媒体等警察情報システム等に接続し情報を入出力する電磁的記録媒体をいう。（機密性低情報のみが記録された読み出し専用のものを除く。）

(15)　情報

入出力資料、ドキュメント又は外部記録媒体若しくは警察情報システム等内部に記録された情報をいう。

(16)　外部回線

警察機関の管理が及ばない電子計算機が論理的に接続され、当該電子計算機の通信に利用されるインターネットその他の電気通信回線をいう。

第２　管理体制

１　情報セキュリティ管理者

情報セキュリティ管理者は、情報セキュリティに係る事務を統括するに当たり、その事務に関係するシステムセキュリティ責任者及びシステムセキュリティ維持管理者の意見を聴き、十分検討した上で処理しなければならない。

２　システムセキュリティ責任者

(1)　警察情報システム等の整備を担当する所属にシステムセキュリティ責任者を置き、それぞれ当該所属長をもって充てる。

(2)　システムセキュリティ責任者は、整備する警察情報システム等に関して、システムセキュリティ維持管理者及び運用管理者が３の(2)及び６の(2)の事務を処理するに当たって必要なセキュリティ要件を当該警察情報システム等が備えるための事務を処理するとともに、整備した警察情報システム等におけるシステムセキュリティ維持管理者が行う事務を統轄する。

３　システムセキュリティ維持管理者

(1)　警察情報システム等を構成する電子計算機及びネットワーク機器の管理者権限

を保有する所属に、システムセキュリティ維持管理者を置き、それぞれ当該所属長をもって充てる。

(2)　システムセキュリティ維持管理者は、担当する警察情報システム等の維持管理時における情報セキュリティに係る事務を処理する。

(3)　システムセキュリティ維持管理者は、その管理する電子計算機及びネットワーク機器ごとにシステム管理担当者及びネットワーク管理担当者を指名し、業務の責務に即した必要な範囲において管理者権限を付与しなければならない。ただし、ネットワーク機器の維持管理に係る事務が軽微であると認められる場合は、ネットワーク管理担当者を指名しないことができる。この場合、ネットワーク管理担当者の事務はシステム管理担当者が行うものとする。

(4)　システムセキュリティ維持管理者は、システム管理担当者及びネットワーク管理担当者の指定状況をシステム・ネットワーク管理担当者指名簿（別記様式第１号）により管理しなければならない。

4　システム管理担当者

(1)　システム管理担当者は、担当する電子計算機その他の警察情報システム等の情報セキュリティに係るシステム管理に関する事務を行う。

(2)　システム管理担当者は、同一の者が複数の電子計算機に関して重複して指名されることを妨げない。

5　ネットワーク管理担当者

(1)　ネットワーク管理担当者は、担当するネットワーク機器その他の警察情報システムに係るデータ伝送に関する監視及び制御その他の情報セキュリティに係るネットワーク管理に関する事務を行う。

(2)　ネットワーク管理担当者は、同一の者が複数のネットワーク機器に関して重複して指名されることを妨げない。

6　運用管理者

(1)　警察情報システム等を運用する所属に運用管理者を置き、所属長をもって充てる。

(2)　運用管理者は、所属における警察情報システム等の運用に関し、情報セキュリティの維持その他の警察情報システム等による処理に係る情報の適正な取扱いを確保するために必要な事務を処理する。

7　運用管理補助者

運用管理者を補助するため、運用管理補助者を置き、県本部の所属にあっては警部の階級又は同相当職の職にある者、署にあっては課長の職にある者を充てる。

なお、当該職にある者がいない部署においては、係長等の職にある者の中から適任者を指定し、明らかにすること。

第３　情報の分類及び取扱い

１　情報の分類

訓令第５条に規定する情報の分類は、別表１のとおり実施する。また、警察情報取扱機器で取り扱われる情報については、別表１の分類に準じて取り扱うものとする。

２　分類が異なる情報の取扱い

機密性、完全性又は可用性のいずれかの情報の分類が異なる情報を一の警察情報システム等で取り扱うことについては、次のいずれかに該当するときに限り認めるものとする。

(1)　当該警察情報システム等において取り扱う情報のうち、最も上位の分類に応じた情報の管理が可能であるとき。

(2)　情報セキュリティ管理者が必要であると認めたとき。ただし、県警察以外の機関が保有主体となる情報については、当該機関の定めるところによる。

３　情報の分類及び通知

(1)　情報セキュリティ管理者は、県警察の警察情報システム等で取り扱われる情報について、当該情報に係る業務を主管する所属長及び当該情報を取り扱う警察情報システム等のシステムセキュリティ責任者と協議の上、分類するものとする。

(2)　情報セキュリティ管理者は、(1)の規定に基づく情報の分類を関係所属長に通知するものとする。

(3)　情報セキュリティ管理者は、情報の分類を変更する必要がある場合には、当該情報に係る業務を主管する所属長及び当該情報を取り扱う警察情報システム等のシステムセキュリティ責任者と協議し、必要な見直しを行わなければならない。

４　情報の取扱い

(1)　一般的な措置

情報の取扱いについては、この項に定めるもののほか、新潟県警察の文書に関する訓令（平成14年本部訓令第８号）に定めるところによる。

ア　情報の作成、入手及び利用

(ｱ)　警察職員（以下「職員」という。）は、情報を不正に作成し、利用し、又は処分若しくはき損してはならない。

(ｲ)　職員は、情報を不当な目的で入手し、複製し、又は他人に提供してはならない。

(ｳ)　職員は、情報を警察の庁舎外に不正に持ち出してはならない。

(ｴ)　職員は、情報セキュリティ管理者が認めた場合を除き、情報の分類を他の者が認識できる方法を用いて明示しなければならない。

イ　情報の管理

職員は、情報の分類に応じて、警察情報システム等、外部記録媒体、ドキュメント並びに入出力資料の紛失及び盗難の防止に対して十分に配意し、適切に管理しなければならない。

ウ　情報の提供

(ｱ)　職員は、情報を公表する場合には、当該情報が別表１において機密性低に分類される情報に分類されるものであることを確認しなければならない。

(ｲ)　職員は、情報を電磁的記録で公表又は提供する場合には、当該情報の付加情報等からの不用意な情報漏えいを防止するための措置をとらなければならない。

エ　情報の消去

(ｱ)　システムセキュリティ責任者は、電子計算機及びネットワーク機器を廃棄し、又は利用を終了する場合には、システム管理担当者又はネットワーク管理担当者に、データ消去ソフトウエア又はデータ消去装置の利用、物理的又は磁気的な破壊等の方法を用いて、すべての情報を復元できないように措置させなければならない。また、システムセキュリティ責任者又はシステムセキュリティ維持管理者は当該情報が復元できないことを確認しなければならない。

(ｲ)　職員は、電子計算機、ネットワーク機器又は外部記録媒体を他の者へ提供する場合には、これらに保存されていた情報を復元できない状態にする必要性の有無を検討し、必要があると認めた情報について、データ消去ソフトウエア、データ消去装置等を用いて、当該情報を復元できないように措置し、システムセキュリティ維持管理者又は運用管理者はこれを確認しなければならない。

(ｳ)　職員は、情報を廃棄する場合には、裁断、データの消去その他の方法により当該情報を復元できないように措置しなければならない。

(2)　情報の分類に応じた措置

情報の分類に応じた措置は、別表２により実施する。

第４　警察情報システム等の構成要素についての対策

１　設置環境、維持管理等

(1)　別表１において機密性高に分類される情報若しくは機密性中に分類される情報に係るデータベース装置若しくはネットワーク機器（施錠された筐体に収容されているものであって電気通信回線から切り離された場合に直ちにそのことが検知できる仕組みを有するもの及び電子計算機（データベース装置を除く。(3)において同じ。）に近接して設置する必要のあるネットワーク機器を除く。）を設置し、又はそれらの装置若しくは機器に係るシステムドキュメントを保管する室（以下「警察情報システム機械室等」という。）は、人及び物の出入りを確実に管理すること

ができ、外部からの侵入及び内部の視認が容易にできない構造の区域としなければならない。また、警察情報システム機械室等には、立入りが認められた者以外の者が立ち入ることができないように必要な措置をとらなければならない。

(2) 情報セキュリティ管理者は、警察情報システム機械室等に立ち入ることができる者の範囲をあらかじめ定め、システムセキュリティ維持管理者又は運用管理者は、そのうち、必要な者に許可を与えなければならない。また、職員以外の者が警察情報システム機械室等に立ち入るときは、職員を立ち会わせなければならない。

(3) 別表１において機密性低、完全性低及び可用性低に分類される情報以外の情報（以下「要保護情報」という。）を取り扱う電子計算機を設置し、それらの機器に係るシステムドキュメントを保管し、又は要保護情報に係る入出力資料及び外部記録媒体を取り扱う場所は、人及び物の出入りを管理することができるように区画された区域とし、電子計算機の画面、システムドキュメント及び入出力資料をその区域の外から視認することができない構造としなければならない。また、その区域には、立入りが認められた者以外の者が立ち入ることができないよう必要な措置をとらなければならない。

(4) 警察情報システム機械室等に設置されている警察情報システム等を構成する機器、外部記録媒体及びシステムドキュメントを警察情報システム機械室等の外に持ち出そうとする者は、システム管理担当者又はネットワーク管理担当者の立会いの下でこれを行い、その状況を記録しなければならない。

(5) システムセキュリティ維持管理者は、警察情報システムの構成又は情報の処理手順の変更その他の維持管理等に必要なドキュメント及び記録簿を整備し、その内容を常に最新のものとしておかなければならない。また、システム管理担当者及びネットワーク管理担当者は、警察情報システムの構成又は情報の処理手順の変更その他の維持管理等に必要な作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行わなければならない。

(6) 情報セキュリティ管理者は、警察情報システム等について一元的に把握し管理するため、必要な事項を記載した台帳を整備しなければならない。

２　電子計算機

(1) 共通対策

ア　職員は、警察情報システム等を構成する機器、外部記録媒体及びドキュメントを適正に管理しなければならない。

イ　職員は、警察情報システム等を構成する機器、外部記録媒体及びドキュメントを他の者に不正に交付し、又は利用させてはならない。

ウ　職員は、情報セキュリティ管理者が認めた場合を除き、警察情報システム等を構成する機器及び外部記録媒体として、個人所有の機器及び外部記録媒体を利用してはならない。

エ　職員は、あらかじめ定められた目的以外の目的で不正に警察情報システム等を利用してはならない。また、情報セキュリティ管理者が認めた場合を除き、警察情報システム等を構成する機器に電子計算機等を接続又は増設し、若しくは警察情報システム等を構成する機器を交換してはならない。

オ　職員は、システムセキュリティ責任者が認めた場合を除き、警察情報システム等を構成する機器の改造を行い、又はソフトウエアの追加、削除若しくは変更をしてはならない。

カ　職員は、情報セキュリティ管理者が認めた場合を除き、警察情報システム等を構成する機器及び外部記録媒体を警察の庁舎外に持ち出してはならない。

キ　システムセキュリティ責任者は、電子計算機（データベース装置を除く。）について、必要な対策をとらなければならない。

ク　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、データベース装置について、許可のない者が容易に操作できないように所要の措置をとらなければならない。

ケ　システムセキュリティ責任者は、電気通信回線を経由してデータベース装置の保守作業を行う場合は、送受信される情報を暗号化する機能の必要性の有無を検討し、必要があると認めたときは、暗号化しなければならない。また、システムセキュリティ維持管理者は、当該保守作業を行う場合には、送受信される情報を暗号化する必要性を検討し、必要があると認めたときは、暗号化しなければならない。

コ　システムセキュリティ責任者は、電子計算機にインストールしてもよいソフトウェア及び警察情報システム等の維持管理に利用するソフトウェアを定めなければならない。また、システムセキュリティ維持管理者は、これに該当しないソフトウェアが稼働していることを認知した場合は、当該ソフトウェアを停止し、利用を定めたソフトウェアであっても、利用しない機能は無効化しなければならない。

サ　システム管理担当者は、データベース装置の時刻設定を正確なものとしなければならない。

シ　システムセキュリティ責任者又は運用管理者は、警察情報システム等について、盗難及び設置場所からの不正な持ち出しを防止するための措置をとらなければならない。

ス　運用管理者は、外部記録媒体を外部記録媒体管理台帳（別記様式第２号）に登載して管理するとともに、定期的に保管状況を確認しなければならない。

セ　運用管理者は、外部記録媒体を保管するときは保管庫に施錠の上、保管させなければならない。

(2)　持ち出し対策

ア　システムセキュリティ責任者は、持ち出し用パソコンに必要な対策をとらなければならない。

イ　職員は、持ち出し用パソコン及び外部記録媒体を庁舎外に持ち出す場合は、持ち出し用パソコン・外部記録媒体持ち出し承認簿（別記様式第３号）により、システムセキュリティ維持管理者又は運用管理者の承認を得なければならない。

ウ　職員は、持ち出し用パソコン及び外部記録媒体を庁舎外に持ち出すことを終了した場合には、持ち出し用パソコン・外部記録媒体持ち出し承認簿により、当該承認者に対してその旨を報告しなければならない。また、当該承認者は、持ち出し期間が満了しているにもかかわらず終了の報告がない場合は、その状況を確認し、必要な対応を講じなければならない。

エ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察の庁舎外で持ち出し用パソコンから無線回線を利用してその他の警察情報システム等にアクセスする仕組みを構築してはならない。

3　システムセキュリティ責任者が講じる措置

(1)　外部記録媒体の利用制限

システムセキュリティ責任者は、職員が許可なく外部記録媒体を利用して情報を入出力できないようにするため、必要な措置を講じなければならない。

(2)　外部記録媒体に記録する情報の暗号化機能の付与

ア　システムセキュリティ責任者は、外部記録媒体に記録する情報を自動的に暗号化する機能（以下「自動暗号化機能」という。）を電子計算機に設けなければならない。

イ　システムセキュリティ責任者は、自動暗号化機能を用いない場合に備え、自己復号型の暗号措置（特定のソフトウエアを使用することなく、あらかじめ設定された文字列を入力することにより暗号化されたファイルの復号が可能となる暗号措置のことをいう。以下同じ。）を行う機能又は当該機能と同等以上のセキュリティ基準を満たすと情報セキュリティ管理者が認める暗号措置を行う機能（以下「自己復号型暗号措置機能等」という。）を電子計算機に設けなければならない。

(3)　外部記録媒体の利用状況の証跡取得機能の付与

システムセキュリティ責任者は、外部記録媒体に対する情報の入出力操作及び外

部記録媒体の利用の許可に関する証跡を取得する機能を電子計算機に設けなければならない。

(4)　電子計算機の内蔵ハードディスクの自動暗号化機能の付与

　システムセキュリティ責任者は、電子計算機の内蔵ハードディスクに記録される情報を自動的に暗号化する機能を当該電子計算機に設けなければならない。

(5)　紛失、盗難等防止対策の実施

　システムセキュリティ責任者は、電子計算機の内蔵ハードディスクに記録された情報が警察部外へ流出することを防止するため、当該電子計算機の紛失、盗難等防止対策を実施しなければならない。

4　外部記録媒体の利用の管理

(1)　外部記録媒体の利用申請

　職員は、外部記録媒体を利用して情報を入出力する必要がある場合には、運用管理補助者に外部記録媒体の利用について申請するものとする。この場合において、職員は、自動暗号化機能を用いて暗号化した情報を復号できない機関等に、情報を移送するため、自己復号型暗号措置機能等を用いて当該情報を暗号化する必要があるとき、又は自己復号型暗号措置機能等を用いないとき（情報セキュリティ管理者が認めたときに限る。(2)及び(3)において同じ。）は、当該事項について併せて申請しなければならない。

(2)　外部記録媒体の利用許可等

　運用管理補助者は、(1)に定める申請があった場合には、業務上の必要性等を審査した上で、必要と認めるときは、必要最小限の範囲で許可するものとする。また、運用管理補助者は、自動暗号化機能又は自己復号型暗号措置機能等を用いずに情報を記録することについて申請があった場合には、状況に応じて、職員に対し、ソフトウェアが有するパスワード保護機能等を活用するなど、情報セキュリティの向上に必要な措置を講ずるよう指示するものとする。

(3)　外部記録媒体への情報の記録

ア　職員は、(2)に定める許可を受けた場合には、自動暗号化機能を用いて外部記録媒体に情報を記録しなければならない。

イ　職員は、アに定めるところにかかわらず、自動暗号化機能を用いて暗号化した情報を復号できない機関等に情報を移送する必要がある場合であって、運用管理補助者の許可を得たときは、自己復号型暗号措置機能等を用いて情報を暗号化した上で記録し、又は自動暗号化機能若しくは自己復号型暗号措置機能等を用いずに情報を記録することができるものとする。この場合において、職員は、運用管理補助者から、情報セキュリティの向上に必要な措置を講ずるよう指示を受けた

ときは、当該措置を講じなければならない。

(4)　対象範囲

３及び４の対象とする範囲は、警察情報システム等を構成する電子計算機（外部記録媒体を含む。）のうち、次に掲げるものを除いたものとする。

ア　データベース装置

イ　データベース装置に係る外部記録媒体

ウ　インターネットに接続された電子計算機

5　外部記録媒体の利用状況に係る検証

(1)　証跡の定期的な検証及び報告

運用管理補助者は、職員の外部記録媒体に対する情報の入出力操作及び外部記録媒体の利用許可に関する証跡を定期的に検証し、その結果を運用管理者に報告しなければならない。

(2)　報告に基づく対応等

ア　運用管理者は、(1)に定める報告に基づき、必要に応じて適切な対応をしなければならない。

イ　運用管理者は、(1)に定める報告について、簿冊等により管理するものとする。

6　電子メール及びウェブ

(1)　職員は、業務遂行に係る情報を含む電子メールを送受信する場合には、警察が運営又は外部委託した電子メール機能を利用しなければならない。また、受信した電子メールについては、適切な方法により当該内容を表示しなければならない。

(2)　システムセキュリティ責任者は、電子メールの送受信時に認証を行う機能を設けなければならない。

(3)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電子メールを保管、送受信又は中継するために設置される電子計算機及びウェブサービスを提供するために設置される電子計算機を不正に使用されることのないように構築し、管理しなければならない。

(4)　職員及びシステムセキュリティ責任者は、電子メール機能の利用及びウェブサービスの提供に当たって、利用者の情報セキュリティが損なわれることのないように必要な措置をとらなければならない。また、職員以外の者に電子メールの送信又はウェブサービスを提供する場合には、情報セキュリティ管理者が認めたドメイン名を使用しなければならない。

7　電気通信回線

(1)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電気通信回線を利用するに当たっては、当該接続による情報セキュリティの維持に係るリス

クを検討しなければならない。

(2)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等を構成する電気通信回線として、情報セキュリティ管理者が認めた回線を利用しなければならない。

(3)　職員は、情報セキュリティ管理者が認めた場合を除き、警察情報システム等を構成する機器を外部回線に接続し、又は外部回線から警察情報システム等にアクセスする仕組みを構築してはならない。

(4)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、ネットワーク機器について、許可のない者が容易に操作できないように所要の措置をとらなければならない。

(5)　ネットワーク管理担当者は、ネットワーク機器の時刻設定を正確なものとしなければならない。

(6)　ネットワーク管理担当者は、警察情報システム等を構成する電気通信回線の監視をシステム管理担当者と協力して行わなければならない。また、監視により得られた結果は、消去や改ざんが行われないように管理しなければならない。

第５　情報セキュリティ要件の明確化に基づく対策

１　情報セキュリティについての機能

(1)　アクセス制御機能等

ア　システムセキュリティ責任者は、アクセス権者以外の者によるアクセス及びアクセス権者によるアクセス範囲を越えたアクセスを防止するために、整備する警察情報システム等ごとに認証、アクセス制御及び権限管理を行う機能を設けなければならない。

　また、アクセス権者及び各アクセス権者のアクセス範囲を定める場合は、当該警察情報システム等で取り扱う情報に係る業務を主管する所属の長と協議の上、整備する警察情報システム等ごとに、必要な手続を明確化したうえで、業務上の責務と必要性を勘案し、必要最小限の範囲に限らなければならない。

イ　職員は、自己のユーザＩＤ以外のユーザＩＤを用いて、警察情報システム等を利用してはならない。

ウ　職員は、自己のユーザＩＤ及びパスワード（以下「ユーザＩＤ等」という。）を他の者に知らせてはならない。また、自己のユーザＩＤ等を他の者に知られないように適切に管理しなければならない。ただし、人事異動、長期休暇等に伴う引継のために特に設定したユーザＩＤ等及びあらかじめ複数の者が共用することをシステムセキュリティ責任者又はシステムセキュリティ維持管理者が認めたものについては、この限りでない。

エ　職員は、ＩＣカード等による認証を用いる場合には、ＩＣカード等を本人が意図せずに使用されることがないように安全措置をとるとともに、紛失しないように管理し、他の者に付与又は貸与してはならない。ただし、あらかじめ複数の者が共有することをシステムセキュリティ責任者又はシステムセキュリティ維持管理者が認めたものについては、この限りでない。また、ＩＣカード等を利用する必要がなくなった場合には、これをシステムセキュリティ維持管理者に返納するなどの適切な措置をとらなければならない。

オ　システムセキュリティ維持管理者は、遠隔地から制御又は監視する警察情報システム等について権限のない者が遠隔地から当該機器の制御又は監視を行うことがないよう厳重に管理しなければならない。

カ　システムセキュリティ維持管理者は、システム管理担当者及びネットワーク管理担当者の権限を、個別の者に付与しなければならない。また、これを他の職員に代理させることはできない。

(2)　証跡管理

ア　システムセキュリティ責任者は、警察情報システム等について、証跡管理を行う必要性の有無を検討し、証跡を取得する必要があると認めた警察情報システム等には、証跡を取得する機能を設けなければならない。

イ　システムセキュリティ維持管理者は、警察情報システム等に設けられた機能を利用して、事象ごとに必要な項目を証跡として記録し、管理しなければならない。また、その記録を必要に応じて分析し、適切な措置をとらなければならない。

ウ　システムセキュリティ維持管理者は、システム管理担当者、ネットワーク管理担当者及び職員に対して、証跡の管理、分析等を行う可能性があることをあらかじめ周知しなければならない。

エ　運用管理者は、所属の警察情報システム等のアクセス権者及びアクセス範囲を適正に管理しなければならない。

(3)　暗号と電子署名

ア　職員は、暗号化された情報の復号又は電子署名の付与に用いる鍵の管理を適切に行わなければならない。

イ　情報セキュリティ管理者は、暗号化又は電子署名の付与に用いることができるアルゴリズムを、別途定めるとともに、当該アルゴリズムの安全性に関する情報を収集し、必要な変更を行わなければならない。

ウ　システムセキュリティ責任者は、警察情報システム等において暗号化又は電子署名の付与に用いるアルゴリズムを情報セキュリティ管理者が定めたものから選定するとともに、暗号化された情報の復号又は電子署名の付与に用いる鍵の管

理について定めなければならない。

エ　システムセキュリティ維持管理者は、電子署名の付与を行う必要があると認めた警察情報システム等について、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供しなければならない。

2　特定脅威等への対策

(1)　セキュリティホール対策

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電子計算機及びネットワーク機器の構築及び運用開始時に、当該機器上で利用するソフトウエアに関連する公開されたセキュリティホールについて対策を講じなければならない。

イ　システム管理担当者及びネットワーク管理担当者は、管理対象となる電子計算機及びネットワーク機器に関連する公開されたセキュリティホールの情報の入手に努めなければならない。また、その情報を入手した場合には、システムセキュリティ責任者及びシステムセキュリティ維持管理者に報告しなければならない。

ウ　システムセキュリティ責任者は、入手したセキュリティホールに関連する情報から、当該セキュリティホールが警察情報システムにもたらすリスクを分析した上で、必要と認めたものに対して、セキュリティホール対策を講じるとともに、随時職員に周知しなければならない。

エ　システムセキュリティ維持管理者は、定期的にセキュリティホール対策及びソフトウエア構成の状況を記録し、これを確認、分析するとともに、不適切な状態にある電子計算機及びネットワーク機器を把握した場合には適切に対処しなければならない。

オ　システムセキュリティ責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、システムセキュリティ維持管理者及び他のシステムセキュリティ責任者と共有しなければならない。

(2)　不正プログラム対策

ア　職員は、コンピュータ・ウイルス等不正プログラムが電子計算機及び外部記録媒体に存在していないことを確認しなければならない。また、不正プログラムが発見された場合には、直ちに拡散の防止のための措置をとらなければならない。

イ　情報セキュリティ管理者は、不正プログラム感染の回避を目的とした職員に対する留意事項を含む日常的実施事項を定めなければならない。

ウ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、不正プログラムから電子計算機（当該電子計算機で動作可能なコンピュータ・ウイルス

対策ソフトウエア等が存在しないものを除く。)を保護するための対策を講じなければならない。また、不正プログラム対策の状況を適宜把握し、その見直しを行わなければならない。

(3)　IPv6技術を利用する通信への対策

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等にIPv6技術を利用する通信（以下「IPv6通信」という。)の機能を導入する場合には、他の警察情報システム等の情報セキュリティが損なわれることのないように必要な措置をとらなければならない。

イ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、IPv6通信を想定していない電気通信回線に接続するすべての電子計算機及びネットワーク機器について、IPv6通信を停止するための機能を有している場合には、当該機能の設定を適切に行わなければならない。

(4)　踏み台対策

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、外部回線に接続する警察情報システム等が、不正アクセス等の中継地点として使用されることを防止するため、(1)及び(2)に掲げるもののほか、必要な措置をとらなければならない。また、不正アクセス等の中継地点として使用された場合の影響が最小となるように警察情報システム等を構築しなければならない。

3　警察情報システム等のセキュリティ要件

(1)　警察情報システム等の計画・設計

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等について、その構築から運用管理にわたり、情報セキュリティを維持することが可能な体制の確保に努めるものとする。

イ　システムセキュリティ責任者は、警察情報システム等のセキュリティ要件を決定し、その要件を満たすために機器等の購入（購入に準ずる賃貸借契約を含む。)及びプログラム開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策並びに警察情報システム等の構成要素についての対策について定めなければならない。

ウ　システムセキュリティ責任者は、構築する警察情報システム等に重要なセキュリティ要件があると認めた場合には、当該警察情報システム等のセキュリティ機能の設計について第三者機関によるＳＴ（Security Target：セキュリティ設計仕様書）評価・ＳＴ確認を受けなければならない。ただし、警察情報システム等を改修する場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときは、この限りでない。

エ　システムセキュリティ責任者は、構築した警察情報システム等の運用を開始するに当たって、情報セキュリティの観点から実施する運用開始のための手順及び環境を定めなければならない。

(2)　警察情報システム等のセキュリティ対策

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等の構築、運用及び監視に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行わなければならない。

イ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等の移行又は廃棄を行う場合は、情報の消去及び保存並びに警察情報システム等の再利用について必要性を検討し、適切な措置をとらなければならない。

ウ　システムセキュリティ責任者は、警察情報システム等の情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置をとらなければならない。

エ　情報セキュリティ管理者は、情報セキュリティ対策が不十分な電子計算機について、システムセキュリティ責任者及びシステムセキュリティ維持管理者に対して必要な指示を行うこと。また、当該システムセキュリティ責任者及びシステムセキュリティ維持管理者は、情報管理課と連携し、速やかに対策を実施すること。

オ　情報セキュリティ管理者は、エの情報セキュリティ対策の実施状況及びその実効性について検証を行うこと。

4　外部委託

(1)　外部委託に当たっては、委託によって情報セキュリティが損なわれることのないように十分に検討の上、委託先には事業継続性を有すると認められる事業者を選定しなければならない。

(2)　システムセキュリティ責任者又はシステムセキュリティ維持管理者は、警察情報システム等の開発、運用管理、維持管理等を外部委託する場合は、あらかじめ当該委託に係る作業を監督する職員の任務を定めるとともに、当該委託に係る業務の実施の場所及び方法、当該委託に係る業務に従事する者の範囲、委託先によるアクセスを認める範囲その他警察情報システム等の情報セキュリティの観点から委託の相手方に遵守させるべき事項を明記した仕様書等を作成しなければならない。また、契約に当たっては、当該事項を遵守させるための措置を定めるなど情報セキュリティの維持に関し所要の措置をとらなければならない。

(3)　システムセキュリティ責任者又はシステムセキュリティ維持管理者は、警察情報システム等に係る仕様書で一般に公開されるものを作成する場合は、当該仕様書が

情報セキュリティの観点から支障のないものであることについて、あらかじめ情報管理課長の確認を受けなければならない。

5　業務継続計画との整合的運用の確保

情報セキュリティ管理者、システムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理者は、業務継続計画（優先度が高い業務の継続性を確保するために必要な事項を定めたものをいう。以下同じ。）を策定する場合には、業務継続計画と警察情報セキュリティポリシーの整合的な運用が可能となるよう必要な措置をとらなければならない。

第6　事案発生時の措置

1　対処方法等の策定及び周知

情報セキュリティ管理者は、障害・事故等の事案について、迅速かつ的確に措置するために必要な事項を定め、職員に周知しなければならない。

2　職員等の責務

システムセキュリティ責任者、システムセキュリティ維持管理者、運用管理者及び職員は、障害・事故等の事案発生時に、情報セキュリティ管理者が定める事項に基づき、必要な措置をとらなければならない。

3　事案の原因調査と再発防止策

システムセキュリティ責任者、システムセキュリティ維持管理者、運用管理者は、障害・事故等の事案が発生した場合には、当該事案の原因を調査し再発防止策を策定しなければならない。また、当該事案の重要性に鑑み、その調査結果を情報セキュリティ管理者に報告しなければならない。

4　警察情報セキュリティポリシー違反時の対応

(1)　情報セキュリティ管理者は、3による報告を受けた事案が、職員が警察情報セキュリティポリシーに違反して警察情報システム等を使用したことによる場合には、期間を　定め、当該職員に警察情報システム等を使用させないことができる。

(2)　情報セキュリティ管理者は、3による報告を受けた事案が、警察情報セキュリティポリシーの違反である場合には、当該警察情報システム等の運用を停止することができる。

第7　教養

情報セキュリティ管理者は、警察情報セキュリティポリシーを正しく理解し、これを確実に実施できるようにするため、職員に対し、職務に応じた教養を行うための体制を整備しなければならない。

第8　その他

1　警察情報セキュリティポリシーに係る情報の管理

職員は、警察情報セキュリティポリシーのうち、公知となることによって警察情報システム等に係る犯罪、不正行為等による情報の漏えいその他の情報セキュリティの侵害事案の発生が懸念され、又は公知となることによって既存の警察情報システム等に新たな情報セキュリティに係る対策を講じる必要が生じるものについては、部外に公開してはならない。

２　警察情報セキュリティポリシーの見直し

警察情報セキュリティポリシーの規定については、見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行わなければならない。

３　細目的事項に関する委任

この要綱に定めるもののほか、警察情報システム等に係る情報セキュリティの維持に関し必要な細目的事項は、別に定めるものとする。

第９　要綱の準用

当分の間、警察業務に係る情報の処理を行うワードプロセッサ（主としてワードプロセッサとしての処理を行う専用機をいう。）及び当該ワードプロセッサで取り扱われる情報を記録した電磁的記録媒体については、警察情報取扱機器及び外部記録媒体として、この要綱第４の２の⑴のアからカまで、シからセまで及び第４の３の⑴並びに第６の規定を準用する。